

**SEALED**

5:18-mj-00071

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Special Agent Christian Bockmann, affiant, do hereby depose and state the following:

1. I submit this affidavit in support of an application for a search warrant for a property located at, 1118 Stagecoach Road, Woodstock, VA, 22664, which has multiple outbuildings on the property. The main structures have a log and wood structure exterior, with wood shingles on the roofs, as described in Attachment A (hereinafter "PREMISES").
2. I am a Special Agent (SA) with the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) and have been so employed since 2009. I am currently assigned to the ATF Martinsburg Field Office, Washington Field Division. Prior to becoming an ATF agent, I was a United States Capitol Police Officer in Washington, D.C., for approximately seven years. In my capacity as a law enforcement officer, I have conducted numerous federal investigations involving illegal possession and use of firearms, and illegal possession and distribution of controlled substances. Many of these investigations led to the arrest and conviction of individuals for violations of both state and federal firearms and drug trafficking laws.
3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

## PROBABLE CAUSE

1. Since approximately October 2017, law enforcement have been investigating narcotics and firearms trafficking within the Western District of Virginia and elsewhere. A Confidential Informant (CI-1) informed Law Enforcement that Katie HARLOW (HARLOW) was distributing illegal narcotics in the area.

2. In 2018, CI-1 was arrested for embezzlement; he is cooperating with law enforcement in return for consideration for his pending charges (herein, CI-1 will be referred to with the masculine pronoun, which is not meant to suggest CI-1's true gender). CI-1 has provided reliable information to law enforcement on numerous occasions.

3. From a period starting on or about April 2018 until the end of July 2018, acting under law enforcement supervision, CI-1 purchased methamphetamine from HARLOW on multiple occasions.

### Controlled Purchase of Methamphetamine on April 4, 2018

4. On or about April 4, 2018, CI-1 contacted KATIE HARLOW about purchasing a pre-determined quantity of methamphetamine. CI-1 subsequently engaged in a controlled purchase, at the direction of law enforcement. Prior to this controlled purchase, CI-1 and the vehicle he was driving ("the CI-1 vehicle") were searched and found to be clear of any illegal contraband. CI-1 was equipped with electronic surveillance equipment for the controlled purchase. During the controlled purchase, HARLOW got into the CI-1 vehicle to carry out the methamphetamine transaction. At the conclusion of the deal, a male walked over to the CI-1 vehicle and was introduced as HODGES, at which time, CI-1, HARLOW, and HODGES engaged in a conversation. In that conversation, HARLOW and HODGES acknowledged that HODGES is a supplier of methamphetamine. After the controlled purchase, CI-1 and the CI-1 vehicle were

searched and cleared of any illegal contraband.

Controlled Purchases of Methamphetamine on April 19, 2018 and April 26, 2018

5. On or about April 19, 2018 and on or about April 26, 2018, at the direction of law enforcement, CI-1 purchased methamphetamine from HARLOW. Prior to and after both controlled purchases the CI-1 and the CI-1 vehicle were searched and found to be clear of any illegal contraband. CI-1 was equipped with electronic surveillance equipment for both controlled purchase.

Cooperating Source of Information

6. On or about November 23, 2018, law enforcement met with a Cooperating Source (CS) who had information about HARLOW trafficking methamphetamine. The CS stated that he is friends with HARLOW and has known her for several years (herein, the CS will be referred to with the masculine pronoun, which is not meant to suggest the CS's true gender). The CS generally stated that HARLOW is one of main suppliers of methamphetamine in Shenandoah County and the surrounding area. The CS also stated that HARLOW has been selling methamphetamine for several years. The CS stated that he has been with HARLOW when she has made a purchase of methamphetamine for distribution.

Search Warrant for Katie HARLOW's Cell Phone

7. Law enforcement searched HARLOW's cell phone pursuant to a state search warrant and found numerous conversations that are consistent with narcotics sales and using narcotics to rent someone's vehicle, as well as pictures taken of suspected methamphetamine and methamphetamine use.

Recorded Conversations from the Rappahannock, Shenandoah, Warren Regional Jail

8. Law enforcement reviewed conversations that involved HARLOW as a participant and which took place either while she was incarcerated, or, while she was out of the Rappahannock, Shenandoah, Warren Regional Jail (RSW Jail), but involved people who were incarcerated there. Since 07/01/2018, Law enforcement reviewed multiple audio files of recorded calls and JPEG text messages from the RSW Jail system which include conversations in which HARLOW discusses her sales and use of narcotics. Included in these messages are conversations with Timmy Theodore, the father of HARLOW's child, with whom she has an on-and-off relationship. In particular, the messages show that HARLOW and Theodore had multiple conversations in the last 60 days from the date of the execution of this affidavit in which the pair discuss how HARLOW needs to stop selling narcotics and using narcotics while she is pregnant, and that she needs to stay away from other people she knows who sell and use narcotics.

9. Audio of recorded RSW Jail calls during this same time period also includes conversations in which HARLOW states she is keeping a large amount of cash at her residence, which belongs to her and another suspected large quantity narcotics trafficker. In contemporaneous messages, HARLOW identified her residence as the 1118 Stagecoach Road, Woodstock, Virginia address.

#### Probable Cause to Search PREMISES for Evidence

10. Approximately two weeks ago, HARLOW represented the 1118 Stagecoach Road address as her residence in a Department of Social Services hearing.

11. As shown in a JPEG text message from the RSW Jail system, on or about November 15, 2018, HARLOW told Timmy Theodore that she is staying at the 1118 Stagecoach Road, Woodstock, Virginia, address.

#### USE OF CELLULAR TELEPHONES/STORAGE MEDIA BY DRUG TRAFFICKERS

8. Based on my training, experience, and participation in narcotic and drug-related investigations, and my knowledge of this case, I know that:

- a. It is common for individuals engaged in the distribution of controlled substances to use telephonic communications, both cellular (to include voice and text messages) and hard line, to further their criminal activities by coordinating the distribution of narcotics, illegal proceeds of narcotics trafficking, and other efforts of co-conspirators;
- b. Individuals engaging in the distribution of controlled substances use cellular telephones and cellular telephone technology to communicate and remain in constant contact with customers and the sources of those controlled substances;
- c. Individuals who engage in the distribution of controlled substances use cellular telephones to exchange information with customers and/or source(s) of supply through text messaging and instant messaging in addition to direct telephone conversations. It is also common for narcotics traffickers to send photographs and videos as exchange of information with customers and/or source(s) of supply; and
- d. Individuals who engage in the distribution of controlled substances frequently maintain information, personal records, photographs, and documents in an electronic format on computers and/or smart phones.

9. In my training and experience, it is likely that the PREMISES will contain at least one cellular phone because of the use of cellular phones in furtherance of the conspiracy to distribute controlled substances described above.

10. I know from my training and experience, as well as from information found in

publicly available materials including those published by cellular phone providers, that some makes and models of cellular phones offer their users the ability to unlock the device via the use of a fingerprint or thumbprint (collectively, “fingerprint”) in lieu of a numeric or alphanumeric passcode or password. This feature is called Touch ID.

11. If a user enables Touch ID on a given cellular phone device, he or she can register fingerprints that can be used to unlock that device. The user can then use any the registered fingerprints to unlock the device by pressing the relevant finger(s) to the device’s Touch ID sensor. In my training and experience, users of cellular phone devices that offer Touch ID often enable it because it is considered to be a more convenient way to unlock the device than by entering a numeric or alphanumeric passcode or password, as well as a more secure way to protect the device’s contents. This is particularly true when the user(s) of the device are engaged in criminal activities and thus have a heightened concern about securing the contents of the device.

12. In some circumstances, a fingerprint cannot be used to unlock a device that has Touch ID enabled, and a passcode or password must be used instead. These circumstances include: (1) when more than 48 hours has passed since the last time the device was unlocked and (2) when the device has not been unlocked via Touch ID in 8 hours and the passcode or password has not been entered in the last 6 days. Thus, in the event law enforcement encounters a locked cellular phone device, the opportunity to unlock the device via Touch ID exists only for a short time. Touch ID also will not work to unlock the device if (1) the device has been turned off or restarted; (2) the device has received a remote lock command; and (3) five unsuccessful attempts to unlock the device via Touch ID are made.

13. The passcode or password that would unlock the cellular phone is not known to law enforcement. Thus, it will likely be necessary to press the finger(s) of the user(s) of the cellular

phone to the device's Touch ID sensor in an attempt to unlock the device for the purpose of executing the search authorized by this warrant. Attempting to unlock the relevant cellular phone device(s) via Touch ID with the use of the fingerprints of the user(s) is necessary because the government may not otherwise be able to access the data contained on those devices for the purpose of executing the search authorized by this warrant.

14. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose fingerprints are among those that will unlock the device via Touch ID, and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device. Thus, it will likely be necessary for law enforcement to have the ability to require any occupant of the PREMISES to press their finger(s) against the Touch ID sensor of the locked cellular phone device(s) found during the search of the Subject Premises in order to attempt to identify the device's user(s) and unlock the device(s) via Touch ID.

15. Although I do not know which of a given user's 10 fingerprints is capable of unlocking a particular device, based on my training and experience I know that it is common for a user to unlock a Touch ID-enabled cellular phone device via the fingerprints on thumbs or index fingers. In the event that law enforcement is unable to unlock the cellular phone as described above within the attempts permitted by Touch ID, this will simply result in the device requiring the entry of a password or passcode before it can be unlocked.



16. Due to the foregoing, I request that the Court authorize law enforcement to press the fingers (including thumbs) of individuals found at the PREMISES to the Touch ID sensor of cellular phones for the purpose of attempting to unlock the device via Touch ID in order to search the contents as authorized by this warrant.

F. TECHNICAL TERMS

17. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. IP Address: The Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.
- b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.
- c. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include cellular telephones, hard



disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

#### G. COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

18. As described above and in Attachment B, this application seeks permission to search for records that might be found at the property described in Attachment A, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media, including a cellular phone. Thus, the warrant applied for would authorize the seizure and search of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

19. *Probable cause.* I submit that if a computer or storage medium, including a cellular telephone, is found at the property described in Attachment A, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently

being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

- c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

20. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium at the property described in Attachment A because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

- b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed,

thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or

consciousness of guilt (e.g., running a “wiping” program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

- c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user’s intent.

21. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the

warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.
- b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data at the property described in Attachment A. However, taking the storage

media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

- c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

22. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

#### CONCLUSION

23. Based upon the foregoing, I submit there is probable cause to believe that Katie HARLOW has engaged in a conspiracy to distribute controlled substances, in violation of 21 U.S.C. §§ 841(a) and 846, and that the property described in Attachment A, contains evidence, contraband, fruits, and/or instrumentalities of these criminal activities, as described in Attachment B.

24. Affiant requests that the Court place under seal this affidavit, as well as the accompanying search warrant application, search warrant, and other related documents, until after the search warrant has been executed.

Respectfully submitted,



---

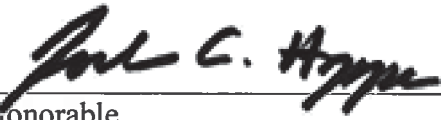
Christian Bockmann



Received by reliable electronic means  
and sworn and attested to by  
telephone on December 6, 2018.

Special Agent (ATF)

~~Subscribed and sworn to before me on December 6, 2018~~

  
\_\_\_\_\_  
The Honorable  
United States Magistrate Judge

## ATTACHMENT A

### *Place to be searched*

Law enforcement has probable cause to believe Katie HARLOW resides at 1118 Stagecoach Rd., Woodstock, VA. Stagecoach Rd. has several structures on the premises. The main building is a two-story log cabin house with wood logs on the first floor and wood sheeting on the second floor. The roof is wood shingle with moss. No building on the premise is marked numerically. There is a wood deck for the second floor located on the two (2) side of the residence and a stone chimney on the three four (3/4) corner. The door opens from right to left and appears to be a wood door set in a wood frame. There are multiple vehicles stored on the property. There are several out buildings behind and to the side of the main building. The second building is two stories with wood vertical siding and a wood shingle roof. The second building is on a hill, west-bound to the four (4) side of the main building described above. There is a wood deck on the one (1) side of this building with access to the first floor. There is also a white out-building and several other small structures on the premises.



## ATTACHMENT B

### *Items to be Seized*

All items constituting evidence and/or instrumentalities of violations of 21 U.S.C. §§ 841(a) and 846 (conspiracy to distribute a controlled substance), including, but not limited to, the following:

- a. Controlled substances, packaging materials, indicia of distribution, records and documents, receipts, notes, ledgers and other papers including any ~~computerized or electronic records including~~ <sup>\*</sup>cellular telephones, relating to the ordering, purchase or possession of controlled substances;
- b. U.S. currency and other illicit gains from the distribution of firearms and/or controlled substances;
- c. Books, records, receipts, notes, ledgers, and other papers including any ~~computerized or electronic records including~~ <sup>\*</sup>cellular telephones, relating to the ordering, purchase or possession of firearms;
- d. Address and/or telephone books and papers, including computerized or electronic address and/or telephone records reflecting names, addresses and/or telephone numbers;
- e. Books, records, receipts, bank statements, and records, money drafts, letters of credit, money order and cashier's checks, receipts, pass books, bank checks, safety deposit box keys and any other items evidencing the obtaining, secreting, transfer, concealment, storage and/or expenditure of money or other assets including, but not limited to, firearms and/or controlled substances;
- f. Documents and papers evidencing ownership of firearms, possession of firearms, storage and location of such assets and facilities to safely store and secure such items, such as safes, to include lock boxes, gun safes, and strong boxes;
- g. Photographs, in particular, photographs of firearms and/or controlled substances and photographs of individuals possessing firearms and/or controlled substances and photographs showing the association of individuals;
- h. Indicia of occupancy, residence, and/or ownership of the premises described herein, including, but not limited to, utility and telephone bills, cancelled envelopes, and keys;
- i. Firearms, including, but not limited to, firearms parts, accessories, holsters, and ammunition;

<sup>\*</sup>in the possession, custody, or control of Katie Harlow

cell phone found in the possession, custody, or control  
For any ~~computer or storage medium whose seizure is otherwise authorized by this warrant,~~  
of Katie Harlow  
~~and any computer or storage medium that contains or in which is stored records or information~~  
that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

- a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
- b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. evidence of the lack of such malicious software;
- d. evidence indicating how and when the COMPUTER was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
- e. evidence indicating the COMPUTER user's state of mind as it relates to the crime under investigation;
- f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- h. evidence of the times the COMPUTER was used;
- i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- k. records of or information about Internet Protocol addresses used by the COMPUTER;
- l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
- m. contextual information necessary to understand the evidence described in this attachment.

~~As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).~~

~~The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.~~

~~The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.~~

During the execution of the search of the PREMISES described in Attachment A, law enforcement personnel are authorized to press the fingers (including thumbs) of <sup>Katie Harlow</sup> ~~individuals found~~ ~~at the PREMISES~~ to the Touch ID sensor of cellular phones found at the PREMISES for the purpose of attempting to unlock the device via Touch ID in order to search the contents as authorized by this warrant.